# ROOT LEVEL REGISTRY RULES,<br>THE MANNER OF ADDING NEW<br>GTLDS TO THE INTERNET

by

Roeland M.J. Meyer, CEO, Morgan Hill Software Company, Inc. (MHSC)

Operator of DNSO.NET

A paper submitted to

Working Group C

ICANN/DNSO

**DRAFT**

8Oct99

Morgan Hill Software Company, Inc.  (MHSC)

(MHSC.COM/MHSC.NET/DNSO.NET)

- Abstract -

# ROOT LEVEL REGISTRY RULES,
# THE MANNER OF ADDING NEW
# GTLDS TO THE INTERNET

Presented by Roeland M.J. Meyer, CEO, MHSC

For a number of years (3) we have been at a deadlock regarding the adding of new TLDs on the Internet. The process has been tainted with much acrimony (a partial history is available at DNSO.NET) among the participants.

This paper attempts to describe what can best be called a root registry. From that description is derived the requirements for a TLD registry. Minimum requirements are stated in both cases. It is arguable that the minimum requirements apply to all registries, at any level. The focus is on registries because the registry (the entity that creates the zone file) is the authority while the zone file is only the implementation.

## - Foreword -

The style of this paper is that of a business white paper, wherein the summary/conclusion is presented first and the supporting evidence, analysis, commentary, and details are presented in the remainder of the body. This allows for rapid executive assimilation while allowing for detailed support and substance. Also, this paper is published in Word2K, HTML, Postscript, and PDF. Text-only is not acceptable because formatting is important to meaning.

On Friday, 17Sep99, Jonathan Weinberg [weinberg@mail.msen.com], the co-chairman of the WG-C working group, of the ICANN/DNSO, requested a position paper from the WG-C participants, as follows. This paper is Morgan Hill Software Company's response to that request.

> October 1 -- WG members must submit initial drafts of position papers. We encourage drafters to include these items: an abstract of the proposal, summarizing the drafters' position and recommendations; a clear statement of the proposal and its rationale; an analysis of who and what systems would be affected; a specific implementation plan; a discussion of the costs and risks of the proposal; and a discussion of the proposal's support in the various stakeholder communities. Drafters, however, are free to develop statements in the form they think best.

TABLE OF CONTENTS

## LIST OF FIGURES

## ACKNOWLEDGMENTS

The author wishes to thank the denizens of the DNS mailing lists, whose material is now archived on MHSC servers. For the past three years (1996-1999) the author has been active on many of these lists and has received much valuable input from that participation and collaboration. The lists are ORSC, IFWP, DOMAIN-POLICY, BWG, DNSO.ORG/WG-C, DNSO.ORG/WG-B, and others. Of particular note, the IFWP list, circa 1998, provided a good forum for the development of many good ideas and principles.

In addition, the author wishes to acknowledge the many attempts at adding new TLDs, including Phil Howard’s GRS system, eDNS, AlterNIC, SuperRoot, ORSC staging root, AURSC, IRSC, and others, for pointing the way and providing much needed empirical data over the past 5 years.

## GLOSSARY

**Word**.

CNO (def) the combined TLD of COM, NET, and ORG

Registrar (def) is an intermediary that works as a selling agent for a registry, usually for a commission.

Registry (def) an online system that registers domains, or other registries, in the domain name system. It is the definitive source of referent data for these systems. This paper does not consider IP-block registries.

Root registry (def) a registry of TLD registries.

Root-server (def) a host configured, using [but not restricted to] IETF RFC 2010 as a guideline, to serve root-zone data to the Internet.

Root-server-cluster (RSC) (def), a group of one or more root-servers configured in a cluster, usually using clustering technology (not RFC 2010 compliant, this is usually done to maintain site specific High-Availability, rather than meeting capacity requirements).

Root-server-site (RSS) (def) a facility housing one or more root-server clusters.

SLA (def) Service Level Agreement.

TLD (def) Top-level domain, such as COM, NET, ORG, and EDU

TLD registry (def) a registry of domains or other registries, registry levels below that of the TLD are simply referred to as "registries"

TLD-server (def) a host configured to serve TLD zone data to the Internet.

TLD-server cluster (TSC) (def), a group of one or more TLD-servers configured in a cluster, usually using clustering technology.

Zone (def)

Zone file (def), from BIND8, the file that is created by the delegated authority for a DNS zone. It is the definitive reference for the content of that zone.

.

Root level registry rules, the manner of adding new gTLDs to the Internet

Roeland M.J. Meyer (mailto:rmeyer@mhsc.com)

## 1 Introduction

This paper takes a view that the primary entity of interest is the registry, whatever level it may be operating in. There exists, today, only one well-known registry, that is the InterNIC. However, it should be noted that even the InterNIC does not run a root-registry (wherein new TLDs can be registered). Thus far, the creation of new TLDs is an inconsistent and irregular ad hoc process, which has been maintained exclusively by the IANA, for historical reasons. The USG/IANA has been negligent in this area and has abdicated this responsibility due to lack of effective activity. The measure of this effectiveness, or lack thereof, is the presence/lack of new TLDs. This is the vacuum, which fuels these debates.

This author takes the view that, before we can create new TLDs, we have to define a root registry context within which these TLDs are valid. Not having such a clearly defined context leads to confusion, ambiguity, and eventual stalemate, as has been happening in the past few years. Some of the best and brightest players, in these debates, have been caught in this confusion.

With regards to the TLD themselves, this author sees no difference between them, from a root-registry perspective (IETF RFC 1591 not with standing, in this context, RFC 1591 is a charter outline). From a purely technical perspective, all TLDs are alike as all charters are upheld by the same, context dependent, legal structures, which the root-registry would be well off leaving alone, as being well beyond root-registry jurisdiction.

With the present churn regarding trademark rulings and issues, it is becoming ever more vital that the registry remove its business operation as far as possible from these contentious issues. The registry should not support any form of arbitration directly or otherwise embroil itself in that political debate. It should require the presentation of a court order, from a court of competent jurisdiction, prior to acting on any of these issues, and otherwise remain strictly neutral. It is the root registry’s prime directive to maintain the stability of its operation, above all else. With this in mind, the only defensible strategy is to follow current legal dictates exactly, not try to make new law or support proponents of making new law, such as WIPO. In short, a root registry should recuse itself from being proactive in these legal issues. It must remain steadfastly neutral.

It is the registry’s business to register names, not to adjudicate them. It is the court’s business to adjudicate. If a court of competent jurisdiction wants to impose some sort of filtering on the names, that the registry will use, then it must do so explicitly, via court orders.

## 2 Summary

MHSC proposes the creation, through contract or direct construction, of a root system. This root system must be wholly owned by ICANN/DNSO. It will also include an operational body, to manage day-to-day operations. This will become known as the ICANN/DNSO root system.

The root-server sites must be entirely owned and operated, leased, or otherwise paid for, by the root registry. The specific reason for this is that it is felt that reliable systems cannot depend on the efforts and good faith of unpaid volunteers.

This system may include all or part of the existing legacy root system (the IANA root system), where it is compliant with this proposal or it can be made to be compliant. This root system will also acknowledge and respect other root systems, negotiate name conflicts, and solve DNS resolution problems.

A vital part of this new root system is a root-registry. The basic function of a root registry is to register other registries. These may be TLD registries or registries for other root systems. In keeping with that primary directive, the root registry needs to define process and structure by which those other registries may be added and under what conditions.

- Develop requirements that a TLD registry MUST meet, a minimum TLD SLA. This SLA must be met on day one of operational birth, on a zero-defect basis.
- Restrict the TLD registry to one TLD until it meets solvency requirements.
- Allow no more than 10 TLD registries, or 20%, whichever is greater, to be on such "probation" at any single point in time.

- After a fixed period, if the registry cannot pass the solvency test, its license gets retracted and becomes available to someone else.

Note that business fail-over, network fail-over, and other redundancy considerations must be considered and allowed for in the minimum SLA. The root registry should mandate the SLA. More importantly, the SLA requirements themselves MUST BE STABLE, this is best achieved by keeping the SLA as simple as possible (KISS).

It further needs to implement that process, in an online system, and publish the results in a root zone file. The primary mechanism for this publication is a root server network, which should be maintained by the root system operators directly. Secondary and tertiary mechanisms must also be implemented to allow flexibility of access to this critical data. This is considered a critical part of the service offering, for a root-registry, and consists of DNS, FTP, HTTPS, SMTP, and SMB protocol-based transfer functions, with appropriate authentication mechanisms.

## 2.1 Basic charter for a TLD registry

Regardless of business model envisioned for a TLD registry, they have the same distribution and support requirements and the implementation software should be almost identical in function. The differences are the business rules and the DNS level, for which the TLD registry is authoritative. The TLD registry also has the same run-time operational requirements as the root registry. TLD registries are differentiated by the TLDs for which they are authoritative.

### 2.2 Other registries

Levels below that of the TLD, for which a TLD is authoritative, may also contain other registries. At this point, a case is being made for a special class of DNS entity, called a public DNS registry. All public registries should be enjoined to support a basic operational SLA. Services should include an SSL Certificate Authority, WHOIS/NICNAMES/LDAP directory services, registration services, and multiple zone file distribution/publication mechanisms. However, operational uptimes requirements may be relaxed at the discretion of the parent registry, for registries below that of the TLD.

## 3 Root registry

TLDs must themselves be registered. The function of the root registry is to register and advertise TLDs (a registry of registries), it is not foreseen that individuals will ever use this service for themselves, unless they are doing so under the auspices of an organization of some sort. Therefore, some privacy considerations may not be properly allowed for, in the event that an individual may try to use this service. This is to allow the proper level of disclosure required for organizations and sole-proprietorships. The operative word here is “advertise”. Some concession may be may towards the privacy of individuals, but if an individual truly wishes to use this service, it is suggested that they do so as an organization or under the auspices of some other legal entity than themselves.

Please note that the foregoing is intended for the root registry only. For registries below that of the TLD, suitable arrangements should be made for protecting the privacy of individual registrants. That is, individuals whom are truly persons and not some other legally constructed entity, whenever persons are allowed to register domain names directly.

## 3.1 Root registry functions

A root registry registers other registries, for entry into the root system. For this purpose, an online registry must be operated. This root registry shall follow a minimum set of policies. Additional policies may also be implemented, but they should purposely be kept minimal.

What the root registry really certifies are registries. Ergo, the certification process primarily focuses on certifying the registry, on the theory that if the registry is stable, the TLDs contained within it are also stable. Likewise, if a TLD destabilizes, then the entire TLD registry and all the other TLDs it contains, becomes suspect.

There are certain services which are either not possible for a non-registry to perform or, if performed by a non-registry, will dilute the service itself, or present an authority/trust dilution for the registry. In the best interests of the Internet, the registry should perform these services. However, this should not be construed as stating that the registry is limited to these service offerings. The registry is free to offer additional services, but not at the expense of these basic services.

### *3.1.1 Registrar support*

Newcomers to the DNS scene are Registrars they are not a registry nor are they domains. They have none of the responsibility of managing a root server network, or maintaining the zone file, but they get to collect more than half the money. In return, all they perform is some customer-facing functions and advertising/marketing stuff. They also provide yet another insulating buffer between the customer and the real registry. In this author's opinion, this is not a good thing for either registry or registrant. It is strictly at the option of the registry whether or not they chose to support registrars.

Because the NSI Shared Registry System (SRS) is proprietary, and is not supported by an open-source reference implementation nor is it supported by a published IETF standard RFC, this author cannot support mandating its use by other registries. Ergo, each registry wishing to support registrars must develop its own SRS, either individually or in concert with other registries.

### *3.1.2 Directory, "whois" and Directory services*

A root registry must operate a directory, listing points of contact for all TLD registries that it contains. This contact information shall include the registrant name, contact name/role, the telephone number, physical contact (mailing address), email address, public key, and URL. It is highly recommended that the NICNAMES/WHOIS protocol be used for this, to insure backward compatibility with existing services. For forward compatibility, an LDAP service, serving the same data, should also be implemented.

### *3.1.3 Certificate authority (SSL)*

The root registry is the primary authenticator for each TLD registry. As such, it is also the only legitimate certificate authority for each registry. Rather than risk the issuance of non-authoritative third-party certificates, with accompanying dilution of authority and trust, the root registry will issue site certificates, to each TLD registry, as required, by that registry's needs. In addition, the root registry will issue one CA certificate per TLD registry, which will be counter-signed, with a root-server CA certificate. Such CA certificates should have a minimum expiry of five years. A basic SSL CA tool-set is available as open-source.

### *3.1.4 Secondary root server services*

The parent registry will operate secondary DNS services for all of the TLD zones registered within it. This will be hosted on separate clusters within each root server site. The primary reason for this practice is that, should the TLD operator fail, without warning, the domains registered within it can still be resolved and their downstream clients will not be abandoned by their TLD registry's business failure.

### 3.1.5 *Certification of legal status*

Only verified legal entities can operate a TLD registry. Although the business model is open, no entity, or majority control of an entity, may be held by persons ever convicted of fraud, extortion, or racketeering, in any jurisdiction. Further, the Registry is admonished to not only be free of wrongdoing, but to remain free of the very appearance of wrongdoing. Given the current political climate, it is acknowledged that the latter may be difficult.

### 3.1.6 *Billing*

The root registry should operate on a positive cash-flow basis (not cost-recovery). Operating and paying for the services, outlined herein, is a non-trivial cost. Further, much ongoing work needs to occur in order to pay the staff, maintain the technology, and improve the service. For this reason, billing should occur on a regular basis. Customarily, this period has been annual. However, this proposal incurs a higher operational cost. A one-time annual recurring fee is suggested, with volume-based monthly surcharges, based on the registration activity volume of the down-stream registries, with the exact amounts to be determined.

### 3.1.7 *Cost issues*

### 3.1.8 *Business models*

It is absolutely clear that no one knows which business model will prevail for any given registry or any given TLD. It is therefore considered that any and all business models are equally valid, whether for-profit or non-profit. It is not the business of the root registry to evaluate business models, or even review them (However, the root registry is not enjoined from offering this as a value-added service offering).

### *3.1.9 TLD Stability and defensibility*

Originally, all TLDs in the Internet had a charter. For many reasons, not all of which are clear, the charters have been allowed to erode for COM, NET, and ORG. The erosion is, at this point, considered irreparable, leading to the current convention that those TLDs are considered equivalent. From now on they are referred to simply as COM/NET/ORG, or CNO.

This creates many problems for members of CNO, not the least of which is the effect of muddying the distinction between the three. A trademark holder can, with reasonable expectation of success, attack a domain in any of those TLDs. There is the additional problem that a new TLD would be vulnerable to similar attack, particularly if the spelling of the TLD should happen to coincide with that of an existing trademark. With recent US PTO rulings (29Sep99), DNS names can definitely not be trademarked at this time. An implication of this is that they should also be proof against trademark infringement, although this remains to be tested in court.

## 3.2 Root registry Requirements for registries

This functions as a registry of registries. This is very unlike a registry of simple domain names, as a more stringent business rule-set must be adhered to. As a publicly visible service (as opposed to a public service), there is an operational stability requirement that registries at lower levels may not have.

In order for the root registry to support the TLD registry, the root registry will require that the TLD registry comply with some basic conditions. This section details those conditions.

### *3.2.1 TLDs should be chartered*

A TLD registry registers domains and other registries for TLDs. A TLD registry may, in fact, register for more than one TLD. However in the initial startup phase, the TLD registry has not proven itself competent, solvent, or stable. Therefore, an initial TLD (one) is granted to the registry for which it must create a charter that TLD will be operated under.[rmjm1]

### *3.2.2 The registry should be a trademark holder*

Legal defensibility is one factor contributing towards stability. TLDs cannot operate under the restraint of legal injunctions. In order to forestall such instability problems it is required that the TLD be associated with a registered trademark or DBA, in whatever jurisdiction the TLD registry will reside, in advance of commencing operations (i.e. "The VPN Registry", with "VPN" as a specific brand, and .VPN as one specific implementation of the mark). While there are no absolutes in the legal world, it is felt that this will increase the likelihood that the TLD operator will prevail in many otherwise threatening legal conditions.[rmjm2]

### *3.2.3 The TLD registry should enforce the charter*

From many viewpoints, including business and legal, there is no point to having a charter that is not enforced. In order to prevent charter erosion, with accompanying erosion of legal defensibility, an enforcement plan must be presented. This plan will be reviewed on the practical merits of enforceability. The cost of the enforcement must be borne by the planner. The plan must include initial reviews of potential registrants, as well as, regular audits of those registrants.

### *3.2.4 Registrants need to be qualified*

The organization that wants to become a registry operator must be a recognized legal entity. Proper identification of the individual, or organization, must be presented and verified. An organization must be legally recognized by their local jurisdiction. Incorporation papers, certificates, or other authentication instruments must be presented. In addition, no entity, or majority control of an entity, may be held by persons ever convicted of fraud, extortion, or racketeering, in any jurisdiction. Certifications to this effect will also be presented.

### *3.2.5 Establish a revenue model*

Although the specific point is built in another part of this document, the operational requirements for a root registry are not inconsequential. This is either borne by higher annual fixed fees charged to the TLD registry, or volume-based fees (some fixed fee per domain name). While this has been universally reviled as an "Internet Tax", there is no other conceivable business revenue model that is nearly as fair to the ultimate registrant. This is ultimately enforceable by the fact that the Root registry will also be running secondary TLD root servers and therefore will have a complete zone file of all of the registered entities in the TLD. Any attempt at fraud will automatically disqualify the TLD registry.

### *3.2.6 Audit/review process*

All registries must comply with a regular (annual) review process that encompasses operations, charter conformance, solvency, reliability, and stability. In the event that the registry is also registering other registries, evidence of their compliance shall be presented during this review.

### *3.2.7 Enter probationary phase*

TLD registries operating their first TLD can only operate that single TLD until they've proven themselves stable and have met the entire minimum SLA for one full year of operation. Special emphasis is placed on the uptime and solvency requirements. If, after the first full-year of operation, the TLD registry is not able to meet the minimum SLA, the TLD registry will be placed on open-bid, while operational control devolves to the root registry and the TLD registry will cease registering new names. If after six months, there is no reasonable bid, for the TLD registry, The customers of the TLD registry will be given the opportunity to either take over the TLD registry, or transfer their names elsewhere. In the latter event, the TLD registry will be dissolved. In either case, a new probationary period will commence.

### *3.2.8 Establish reliable operations*

Full operation, for a TLD registry and TLD root server system, is defined as meeting the published SLA, including 99.99% system-wide uptime requirements, for one full year. Root registries and alternative root systems must meet 99.999% system-wide uptime requirements. All registries downstream from the TLD, need to meet 99.9% annual uptime requirements. Outages involving only a portion of the system (earthquake, fire, flood, and storm), that do not effect the rest of the system shall not count against the system-wide calculations.

## 4 Architectural considerations

One of the principle reasons for much of the dispute over the past years is a discontinuity, between the participants, on how the DNS is to be viewed. There are those idealists that view the original architecture as gospel and advocate forcing deviations to comply with it. There are those that see definite improvements in some of the new forms and wish to go forward with them, experimentally. There are others, of a more practical nature, that simply wish to go forward, from where things are today, and apply the principles to the needs of the growing Internet community. This author is of the latter view.

Multipart root systems and root system networks are now well proven and they are being used today. Every organization, using NAT’d address space, with internal (firewall protected) DNS, is implementing a multi-part root system network using RFC 1918 addresses and both internal and external root systems. These are very large corporations that have definitely solved the scalability problems.

### 4.1 Root systems, hierarchies, and networks

The current DNS system is configured to be hierarchical in nature. There is sufficient argument that this presents an inherent weakness, in terms of centralized control, vulnerability to capture, and some rather severe failure modes. (If one is in Mexico and the data centers in Atlanta, El Paso, and San Diego go offline, then Mexico has no root service and the entire Mexican Internet infrastructure will collapse unless they are already running local root servers, which they are). The reality is that this hierarchical structure is only extant in documents and theory.

Historically a parallel architectural evolution occurred with database schema design. At one time the CODASYL standards were considered to be the epitome of modern database design. This was a purely hierarchical standard. The problem is that, while nice and pretty, it did not meet the needs of its users. Network database schemas, in many cases using the same CODASYL methods, slowly superceded this. This eventually evolved into modern RDBMS and ORDBMS schema design. The migration path is lead by the fact that a hierarchical system is a strict subset of a network system.

Similarly, the DNS system need not remain exclusively hierarchical and in fact, it isn t. The evolution has begun some time ago. For many reasons, having to do with failure-mode compensation, many large service providers use their own copy of the root zone, without referring to the root server system at all. In addition, many additional TLDs are currently in the system, using root servers that are not a part of the formal Internet root server system. Each one of these represents a different root zone authority and independent root system, and they are all interlinked into a fairly robust informal network. [rmjm3]This step alone breaks the strict hierarchical architecture and makes the entire DNS system a network of differing root systems. This paper does not seek to argue with, or deny, reality. The intent here is to work with what we have before us. There is ample proof extant that these conditions are true.

### 4.2 Software standards

Compliance to certain minimum standards will be enforced. This is to assure maximum interoperability between registry and customers/users.

The single most important software package that the registry must operate is that which supports the DNS system and provides interoperability to other registries. While use of proprietary software is allowed, the reference standard is BIND-8.2 and whatever software the registry uses must be 100% compliant with the standards that BIND implements. Sub-implementations will not be tolerated, whereas enhanced features will be allowed, provided that they do not present interoperability problems with BIND-8.2. The reference authority, for BIND, is the IETF[rmjm4].

### 4.3 The relationship of registries to domain names

TLD Registries support TLDs. Without TLD registries, TLDs would not exist. The TLD registry is the sole authoritative source of the TLD zone file. The basis for these statements is the supposition that the registry implements the TLD root servers and supports registration services for a TLD. The current exemplar for this is the InterNIC, which implements both the root servers and the TLD-root servers for COM/NET/ORG. This indicates that there is a one-to-many relationship between registries and TLDs (Registry->TLD). It is also true that, root registries point to TLD registries and there is nothing stopping more than one root registry from pointing to a TLD registry. A TLD registry also does not point back to a root registry unless it wants to refer to another TLD root server. This implies a many to one relationship between root server and TLD root servers (RootServer>-TLDServer).

### 4.4 Registry interoperability with other registries

The ICANN/DNSO, in conjunction with the IETF, will be responsible for developing an open-source Shared Registry System, similar in functionality to that developed by NSI. The NSI SRS is a proprietary system and, as such, is unsuitable for mandated use.

### 4.5 Name conflicts and Addressing

Each registry is responsible for providing working name-space collision avoidance mechanisms within the zone file for which they are authoritative.

There has been very little discussion about private registries in the public forums. Almost all the discussion involves public registries. However, it has been found that there is a certain level of interaction between public and private DNS names, an interaction that has largely been ignored. The particular case is that a private local DNS name is able to mask a public name.

This is exclusively a problem with organizations that have large internal NAT’d address space, with its own internal DNS. A public DNS name, that matches the internal name, will be invisible to the internal organization. For many organizations this is an undesirable side effect. However, this effect may actually be desired, within certain restrictive organizations. Be that, as it may, it is desirable that this only occurs under controlled conditions, rather than by accident.

For this reason, allowances must be made to register a private registry and to excuse that registry from the requirements of the public registries.

### 4.6 Multi-homed and geo-physically separated TLD root server sites

The primary implementation mechanism of the root registry is the root servers. The root servers must be globally visible at all times, on a 24x7 basis. Minimum system-wide uptimes exceeding 99.99% are expected as normal. In order to accomplish this throughout the world, it is recommended that the registry operate at least two separate root-server sites per continental landmass, physically located on each continental landmass, with sufficient separation between them. In addition, each root server site should be multi-homed, via two separate links, to the Internet backbone.

The root-server sites must be entirely owned and operated, leased, or otherwise paid for, by the root registry. The specific reason for this is that it is felt that reliable systems cannot depend on the efforts and good faith of unpaid volunteers. This practice both abuses the volunteer and reduces the control available, to the root registry, over its root servers.

## 5 Business and revenue model

After the first year of operation, the Root registry will not have more than 50% of its TLDs on such probation at any one time. All TLDs will fall under an annual audit that determines minimum SLA compliance.

Page: 12

[rmjm1]It is hoped that a charter would clarify and strengthen the standing of a TLD under trademark dilution attack.

Page: 12

[rmjm2] Recent (29Sep99) US PTO  rulings may make this moot. However, in jurisdictions, outside of the USA, it may be quite effective. Evenso, the recent PTO rulings have yet to be tried in court.

Page: 16

[rmjm3]MHSC has been operating such a system since 1993 and has, in fact, never actually used the legacy IANA root-server system directly and has only been in the DNS system since 1995. This is because MHSC.NET originally started as a ghosted UUCP-style environment. Since then MHSC has added alternate TLD support and, in fact, has its own root system, independent of that run by NSI. This system can be partially accessed via the NS[1-3].MHSC.NET name servers.

Page: 16

[rmjm4]This is in spite of the fact that MHSC frequently disagrees with, and ignores, the IAB. MHSC does not consider the IAB definitive, on architectural issues. MHSC does consider the BIND-master, Paul Vixie, to be authoritative for implementations of BIND.